Daniel Srourian, Esq. (SBN 285678)
SROURIAN LAW FIRM, P.C.
468 N. Camden Dr., Suite 200
Beverly Hills, CA 90210
Telephone: (213) 474-3800
Fax: (213) 471-4160
Email: daniel@slfla.com

Attorney for Plaintiff and
The Proposed Class

UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

DEBORAH CALLEN. individually and on behalf of all others similarly situated,

Plaintiff,

v.

NORTHBAY HEALTHCARE CORPORATION

Defendant.

Case No.:

COMPLAINT – CLASS ACTION

FOR DAMAGES, INJUNCTIVE RELIEF, AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE,**
2. **NEGLIGENCE *PER SE*,**
3. **BREACH OF IMPLIED CONTRACT,**
4. **UNJUST ENRICHMENT,**
5. **VIOLAITON OF CALIFORNIA'S CONSUMER PRIVACY ACT,**
6. **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW,**
7. **VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT.**

JURY TRIAL DEMANDED

Plaintiff Deborah Callen ("Plaintiff") individually and on behalf of all others similarly situated, by and through her undersigned counsel, brings this Class Action Complaint against NorthBay Healthcare Corporation ("NorthBay" or "Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII"[1]) and Protected Health Information ("PHI") (collectively, "Private Information") that was impacted in a data breach that Defendant publicly disclosed in January 2025 (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is a nonprofit healthcare organization headquartered in Fairfield, California, that provides 24-hour emergency care, intensive care, acute care, and advanced surgical and diagnostic services.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. On February 23, 2024, Defendant discovered a security incident on its IT Network. In response,[3] Defendant launched an investigation and engaged third-party cybersecurity experts to determine the nature and scope of the incident.[4]

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *About us*, NORTHBAY HEALTHCARE CORPORATION, https://www.northbay.org/about/index.html (last visited January 30, 2025).

[3] *Exhibit 1*: Deborah Callen Notice Letter.

[4] *Id.*

6. Defendant's investigation determined that an unauthorized third-party gained access to the company's systems between January 11, 2024, and April 1, 2024.[5]

7. Defendant then launched a comprehensive review of the incident to determine the exact type of information compromised as well as identify the individuals affected in the data breach.[6]

8. Upon information and belief, Defendant's investigation determined that the following types of Private Information were compromised in the Data Breach: name, date of birth, Social Security number, passport number, financial account number, medical information, biometric information, health insurance information, driver's license number, state or other government-issued identification number, username and password, and, credit or debit card number, including the expiration date, security code, and/or PIN.[7]

9. On January 29, 2025, Defendant made a public disclosure of the Data Breach and started sending notice letters to impacted individuals.[8]

10. Defendant failed to take precautions designed to keep individuals' Private Information secure.

11. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

12. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

13. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have

---

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Data Breach Notifications*, NorthBay Healthcare Corporation, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/88fc9df0-3e37-449b-81ca-4f5dfebb7385.html (last visited January 30, 2025).

lost the ability to control their private information and are subject to an increased risk of identity theft.

14. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

15. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

16. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

17. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

18. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

19. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

Plaintiff

20. Plaintiff Deborah Callen is a resident of Hercules, California. On January 29, 2025, Defendant sent Plaintiff a notice letter informing her that her Private Information was compromised in the Data Breach. As a result of the Data Breach, Plaintiff has experienced an uptick in spam calls and text messages, and has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, Plaintiff is now subject to substantial and imminent risk of future harm. Plaintiff would not have used Defendant's services had she known that it would expose her sensitive Private Information.

Defendant

21. Defendant is a nonprofit healthcare organization headquartered in Fairfield, California, having its principal place of business located at 1200 B. Gale Wilson Boulevard, Fairfield, California 94533.[9]

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount of controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members, and at least one Class Member is a resident of a different state than Defendant.[10]

23. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District and conducts substantial business in this district. It has also

[9] *Contact us*, NORTHBAY HEALTHCARE CORPORATION, https://www.northbay.org/patients-visitors/location-directions-directory.html (last visited January 30, 2025).

[10] *Data Breach Notifications*, NorthBay Healthcare Corporation, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/88fc9df0-3e37-449b-81ca-4f5dfebb7385.html (last visited January 30, 2025).

conducted systematic and continuous activities in California; and there is a substantial nexus between the conduct Defendant directs at California and the claims asserted herein.

24. Venue is proper in this Court because Defendant is headquartered in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

25. Defendant is healthcare organization that provides 24-hour emergency care, intensive care, acute care, and advanced surgical and diagnostic services.[11]

26. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[12]

27. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

29. On February 23, 2024, Defendant discovered a security incident on its IT Network. In response.[13] Defendant launched an investigation and engaged third-party cybersecurity experts to determine the nature and scope of the incident.[14]

30. Defendant's investigation determined that an unauthorized third-party gained access to the company's systems between January 11, 2024, and April 1, 2024.[15]

---

[11] *About us*, NORTHBAY HEALTHCARE CORPORATION, https://www.northbay.org/about/index.html (last visited January 30, 2025).
[12] *Privacy Policy*, NORTHBAY HEALTHCARE CORPORATION, https://www.northbay.org/patients-visitors/website-privacy-policy.html (last visited January 30, 2025).
[13] *Exhibit 1*: Deborah Callen Notice Letter.
[14] *Id.*
[15] *Id.*

31. Defendant then launched a comprehensive review of the incident to determine the exact type of information compromised as well as identify the individuals affected in the data breach.[16]

32. Upon information and belief, Defendant's investigation determined that the following types of Private Information were compromised in the Data Breach: name, date of birth, Social Security number, passport number, financial account number, medical information, biometric information, health insurance information, driver's license number, state or other government-issued identification number, username and password, and, credit or debit card number, including the expiration date, security code, and/or PIN.[17]

33. On January 29, 2025, Defendant made a public disclosure of the Data Breach and started sending notice letters to impacted individuals.[18]

34. Plaintiff's claims arise from Defendant's failure to safeguard her Private Information and failure to provide timely notice of the Data Breach.

35. Defendant failed to take precautions designed to keep individuals' Private Information secure.

36. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

37. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

38. Defendant admits that unauthorized third persons accessed its network systems. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

---

[16] *Id.*
[17] *Id.*
[18] *Data Breach Notification*, NorthBay Healthcare Corporation, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/88fc9df0-3e37-449b-81ca-4f5dfebb7385.html (last visited January 30, 2025).

39. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

40. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[19] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present patients' sensitive Private Information.

41. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[20] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

42. Here, Defendant waited nearly a year after being made aware of the Data Breach to notify impacted individuals.

D. The Harm Caused by the Data Breach Now and Going Forward

43. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[21]

44. The type of data that may have been accessed and compromised here – such as, names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access.

45. Plaintiff and Class Members face a substantial risk of identity theft given that their Social Security numbers were compromised in the Data Breach. Once a Social Security number

---

[19] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited January 30, 2025).

[20] *Id.*

[21] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited January 30, 2025).

is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

46. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

47. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[22]

48. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[23] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[24] As data breaches continue to reveal, "PII about employees, clients and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[25]

49. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[26] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[27]

---

[22] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited January 30, 2025).

[23] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited January 30, 2025).

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited January 30, 2025).

50. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

51. The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director of the cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[29]

52. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[30]

53. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[31] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant notified impacted people nearly a year after learning of the Breach.

54. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity

---

[28] *Id.*

[29] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited January 30, 2025).

[30] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited January 30, 2025).

[31] *Id.*

theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

55. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

56. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

57. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing

credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

58. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> **Nationwide Class**
> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in January 2025 (the "Class").
>
> **California Subclass**
> All individuals residing in the State of California whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in January 2025 (the "California Subclass").

59. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

60. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

61. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

62. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates

that the Class is comprised of hundreds of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

63. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had her Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and her claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

64. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

65. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

66. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure its past and present patients' Private Information;

i. Whether Defendant was unjustly enriched; and

j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

67. Information concerning Defendant's policies is available from Defendant's records.

68. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

69. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

70. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

71. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

72. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 19 and paragraphs 24 through 57 as though fully set forth herein.

73. Plaintiff brings this claim individually and on behalf of the Class Members.

74. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

75. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

76. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

77. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its current and former patients', Private Information.

78. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

79. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

80. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

81. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

82. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

83. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

84. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

85. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the personal patient information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

86. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

87. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

88. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

89. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

90. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

91. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

92. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 19 and paragraphs 24 through 57 as though fully set forth herein.

93. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

94. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

95. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

96. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

97. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

98. As a result of Defendant's negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

99. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 19 and paragraphs 24 through 57 as though fully set forth herein.

100. Plaintiff and Class Members conferred a benefit upon Defendant by using Defendant's services.

101. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information, as this was used for Defendant to administer its services to Plaintiff and the Class.

102. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant or utilized its services had they known Defendant would not adequately protect their Private Information.

103. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

104. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 19 and paragraphs 24 through 57 as though fully set forth herein.

105. Plaintiff and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining services from Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

106. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

107. Defendant accepted possession of Plaintiff and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

108. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

109. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

110. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

111. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

112. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

113. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff and Class Members' Private Information would remain protected.

114. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

115. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

116. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

117. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

118. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

119. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

120. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

121. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) nominal

damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

122. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

123. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100 *et seq.*
(On Behalf of Plaintiff and the California Subclass)

124. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of herself and the California Subclass (the "Class" for the purposes of this count).

125. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

126. Defendant is a "business" under § 1798.140(b) in that it is a business organized for profit or financial benefit of its owners.

127. Plaintiff and Class Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

128. The personal information of Plaintiff and the Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

129. Defendant knew or should have known that its vendors' computer systems and data security practices were inadequate to safeguard the Class Members' personal information and that the risk of a data breach or theft was highly likely.

130. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff and Class Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

131. As a direct and proximate result of Defendant's acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the loss of Plaintiff and Class Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

132. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

133. On February 5, 2024, Plaintiff's counsel sent a CCPA notice letter to Defendant's registered service agents via mail. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

134. Accordingly, Plaintiff and the Class Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

COUNT VI
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, et seq.
(On Behalf of Plaintiff and the California Subclass)

135. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 19 and paragraphs 24 through 57 as though fully set forth herein.

136. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

137. Defendant violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

138. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and Subclass Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Defendant failed to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any

utility, is unfair when weighed against the harm to Plaintiff and Subclass Members, whose Private Information has been compromised.

c. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. Defendant's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused.

e. Defendant engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

139. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, and California common law.

140. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Member Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk

of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information including duties imposed by the FTC Act, 15 U.S.C. § 45; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code § 1798.80, et seq., and § 1798.81.5, which was a direct and proximate cause of the Data Breach.

141. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of individuals Private Information.

142. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment

for Defendant's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

143. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair and unlawful business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT VII
CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, et seq.
(On Behalf of Plaintiff and the California Subclass)

144. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 19 and paragraphs 24 through 57 as though fully set forth herein.

145. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information [PII] from unauthorized access, destruction, use, modification, or disclosure."

146. Defendant is a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiff and Class Members.

147. Businesses that own or license computerized data that includes PII are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information [PII] that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

148. Defendant is a business that owns or licenses computerized data that includes "personal information" [PII] as defined by Cal. Civ. Code § 1798.80.

149. Plaintiff's and Class Members' PII includes "personal information" as covered by Cal. Civ. Code § 1798.82.

150. Because Defendant reasonably believed that Plaintiff's and Class Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

151. Defendant failed to fully disclose material information about the Data Breach in a timely manner.

152. By failing to disclose the Data Breach in a timely manner, Defendant violated Cal. Civ. Code § 1798.82.

153. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and Class Members suffered damages, as described above.

154. Plaintiff and the Class Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

155. Plaintiff and the Class Members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their Private Information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and her counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: February 5, 2025

By: */s/ Daniel Srourian*

Daniel Srourian, Esq. (SBN 285678)
SROURIAN LAW FIRM, P.C.
468 N. Camden Dr., Suite 200
Beverly Hills, CA 90210
Telephone: (213) 474-3800
Fax: (213) 471-4160
Email: daniel@slfla.com

Courtney Maccarone*
Mark Svensson*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com
Email: msvensson@zlk.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice* forthcoming